

SIKKIM



GOVERNMENT

GAZETTE

**EXTRAORDINARY
PUBLISHED BY AUTHORITY**

Gangtok

Thursday 01st October, 2020

No. 203

GOVERNMENT OF SIKKIM

DEPARTMENT OF INFORMATION TECHNOLOGY

Sectt. Annexe I, Top Floor, Sonam Tshering Marg, Gangtok-737101, Sikkim.

Phone No. (03592)202601, Tele-Fax (03592)207426, Email: dit-sik@nic.in

No. 621/DIT/2020/07

Dated: 29/09/2020

NOTIFICATION

Sikkim Data Protection Policy, 2020

The purpose of formulation of Sikkim Data Protection Policy is to provide sets of guidelines for the maintenance and safety of data stored in or originating from the territorial jurisdiction of Sikkim State. This policy shall be for a period of 5 years.

I. Introduction

Data protection means to protect person or business data and to protect the fundamental rights and freedoms of the person/organisation related to that data. **Data protection** is also safeguarding including physical means, of the important information from corruption, compromise or loss. The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates. There is also little tolerance for downtime that can make it impossible to access important information.

The term *data protection* is used to describe both the operational backup of data and business continuity/disaster recovery. Data protection strategies are evolving along two lines: **data availability** and **data management**. *Data availability* ensures users have the data they need to conduct business even if the data is damaged or lost. *Data management* is an administrative process that includes acquiring, validating, storing, protecting, and processing required data to ensure the accessibility, reliability, and timeliness of the data for its users.

II. Definition

- i. "Data Centre" means any organization, Government or Private within the territorial jurisdiction of the State of Sikkim which store and share applications and data. It comprises components that include switches, storage systems, servers, routers, and security devices.

- ii. "Personal Data" means any information that relates to a natural person, which either directly or indirectly, in combination with other information available,
- iii. "Business Data" means all **data** and personal information accessed, processed, collected, stored or disseminated by business organization in connection with any of the **business** and/or the transferred assets, including any Personally Identifiable Information.
- iv. "Sensitive Data" means **data** consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic **data**, biometric **data**, **data** concerning health or **data** concerning a natural person's sex life or sexual orientation or password.
- v. "Responsible Person" means the person who will be in charge of the data protection of the DC.
- vi. "Register of Systems" means a register of all systems or contexts in which personal data is processed by the Data Centre.

III. Why This Policy ?

- i) The Indian IT act 2000 under section 43A and 72A protect the individual data provided over an technological interface. However it has been felt that a robust data protection policy to be in placed to ensure protection against the dangers posed to an individual's/organisation privacy by state and non-state actors in the information age.
- ii) This data protection policy ensures :
 - a) Safeguard and make available data under all circumstances
 - b) Protects the rights of staff, customers and partners
 - c) Transparency in storage and processing of individuals'/ organisation data
 - d) Protects itself from the risks of a data breach.
 - e) Maintain robust Disaster Recovery mechanism if need arise to provide high uptime of data availability

IV. Who is covered ?

All data centres physically set up/maintained by any organisation, private or government within the jurisdiction of Sikkim State will be covered by the policy. All data collected from the inhabitants of Sikkim or of the State's resources which are stored within the jurisdiction of State or outside or back up outside the State shall also be covered.

V. Manpower setup and its Role

Everyone who works for or with DC has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles data must ensure that it is handled and processed in line with this policy and data protection principles. For the purpose:

Principal Secretary/Secretary, Department of Information Technology, Government of Sikkim shall be the Chief Information Security Officer (CISO). He/she shall have responsibility for overseeing policy implementation with regard to compliance.

All Data Protection Officer/Project Manager of the DCs shall supervise and oversee all the technical aspect of data protection policy /disaster recovery operations. He shall also:

1. Make sure that all necessary guidelines are followed as per the ISO guidelines of International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System -Requirements".
2. Supervise in maintaining all Technical Documents, Official Documents, and Logs etc of the DC.
3. Conduct routine, **Disaster recovery testing (DRP)** to assure that information technology (IT) systems will be restored if an actual **disaster** occurs.

*VII. Lawful,
fair and
transparent
processing*

- i. DC shall ensure its processing of data is lawful, fair and transparent, the DC shall maintain a Register of Systems.
- ii. The Register of Systems shall be reviewed annually.
- iii. Individuals have the right to access their personal data and any such requests made to the DC shall be dealt with in a timely manner.

*VIII. Security
requirements*

- i. The DCs shall follow all the listed guidelines of International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System Requirements".
- ii. Data Centres shall audit their security practice and standards from the State Data Centre annually.
- iii. Data Centres shall ensure all physical security measures within and outside the premises and its surrounding using a security camera,biometric, security guard and any other measures to provide utmost security 24/7.
- iv. Strict access shall be followed by all Employees, Contractors, consultants, partners of organization and its subsidiaries and all visitors inside the DCs.

*IX. Data
protection
guidelines*

- i. Every DCs shall appoint Data Protection Officer/Project Manager who shall be responsible for the data protection and security of data stored in the concerned DC.Data Protection Officers/Project Managers shall be reporting to the CISO as and when required.
- ii. Chief Information Security Officer (CISO) shall be responsible for date security of all the data stored in different data centres set up in the jurisdiction of the State.
- iii. Any organisation Government or Private who wish to set up physical DC shall take the permission from CISO stating the purpose of the creation of data.
- iv. For setting up of virtual data centre(s) through cloud or for using the service of the existing cloud service whose physical server is outside the State or country permission from the CISO has to be obtained stating the purpose of creation of data and for storing outside the State.

- v. Data will only be used for the work or business for which the data has been created by the organisation. Any other use of the data shall only be done with the permission of the CISO.
- vi. Access to confidential information/data of the self may only be given by the Data Protection Officer provided he is convinced that the data is not to be misused.
- vii. All **DCs** will provide regular training to all employees to help them maintain and protect data.
- viii. Regular health check up of the DCs shall be conducted, also examining the functioning of the physical protection means like **CCTV, power back up, A/C** and disaster recovery mechanism adopted by the DCs' and report in writing to CISO annually.
- ix. Data centres shall be updated with patches/updates regularly on the IT infrastructure including servers, Operating System, Databases, application related, network equipment and the storage system, protecting the resources from known issues/threat.
- x. Any security threat felt by the DCs shall be immediately reported to the CISO.

X. *Disclosing data for other reasons* i. In certain circumstances, the Data Centres can allow personal data to be disclosed to law enforcement agencies without the consent of the data subject; however this is to be done with the approval of the CISO.

XI. *Disaster recovery and Business Continuity Plan*

- i. Disaster recovery and business contingency plan should be developed for each DCs and get approved from the CISO. The recovery/backup data shall be stored at different seismic zones of the State or outside the State with the permission of CISO.
- ii. Data Centre Infrastructure should be built following strict guidelines of the Telecommunications Industry Association (TIA 942), American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) guidelines and Fire Protection (NFPA 3) Guidelines.
- iii. Data Centres shall follow practices for application, IT infrastructure, network and data as per IDCA standards.
- iv. Backup plan should be in place to back up the data from online machine to offline device. Database consistency check utility must be run to verify the data backup is consistent and can be used confidentially to recover the data at the time of crisis.
- v. Data replication between Data Centre and Disaster Recovery site should be done by replicating the transaction logs that would be restored automatically at the DR site supporting near-real-time data availability at the DR site.

XII. *Breach* i. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, Data Center shall promptly assess the risk to people's rights and freedoms and if appropriate shall report this breach to the Cyber Crime Cell with copy of information to CISO.

XIII. *Rights of the i.
State
Government*

- i. The State Government reserves the right to amend any provision(s) including amendment or withdrawal of any of the provision/condition as and when necessary in the interest of the State Government and public from time to time under the provision of this Policy.
- ii. The decision of the IT Department, Government of Sikkim, as regards interpretation of this policy shall be final.

**G.P. Upadhyaya, IAS
Additional Chief Secretary,
Department of Information Technology
File no.GoS/621/DIT/2020**